UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF FLORIDA

NICHOLAS PIERCE and MISTY HUNTER, on behalf of himself and all others similarly situated, Plaintiffs, v. **ZEROED-IN TECHNOLOGIES, LLC,** Defendant.	Case No. JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiffs, Nicholas Pierce and Misty Hunter ("Plaintiffs"), individually and on behalf of all similarly situated persons, allege the following against Zeroed-In Technologies, LLC ("Zeroed-In" or "Defendant") based upon personal knowledge with respect to themselves and on information and belief derived from, among other things, investigation by their counsel and review of public documents as to all other matters:

I. INTRODUCTION

1. Plaintiffs bring this class action against human resources ("HR") data analytics company, Zeroed-In Technologies, for its failure to properly secure and safeguard Plaintiffs' and other similarly situated Zeroed-In clients', including Dollar Tree and Family Dollar, employees' personally identifiable information ("PII"), including employees' name, date of birth, and Social Security numbers (the "Private Information"), from criminal hackers.

2. Zeroed-In, based in Fort Myers, Florida, is a data and technology consulting firm that serves more than 70 corporate clients and their employees consisting of more than 1.9 million affected individuals throughout the United States.

3. On or about November 27, 2023, Zeroed-In filed an official notice of a hacking incident with the Maine Attorney General's Office.

4. On or around the same time, Zeroed-In also sent out data breach letters (the "Notice") to individuals whose information was compromised as a result of the hacking incident.

5. Based on the Notice sent to Plaintiffs and "Class Members" (defined below), unusual activity was detected on some of its computer systems on August 8, 2023. In response, Defendant launched an investigation. Zeroed-In's investigation revealed that an unauthorized party had access to certain files that contained sensitive client employee information, and that such access took place between August 7, 2023, and August 8, 2023 (the "Data Breach"). Yet, Zeroed-In waited nearly *four months* to notify the public that they were at risk.

6. As a result of this delayed response, Plaintiffs and Class Members had no idea for approximately *four months* that their Private Information had been compromised, and that they were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm. The risk will remain for their respective lifetimes.

7. The Private Information compromised in the Data Breach contained highly sensitive clients' employees' data, representing a gold mine for data thieves. The data included, but is not limited to, Social Security numbers that Zeroed-In collected and maintained.

8. Armed with the Private Information accessed in the Data Breach (and a head start), data thieves can commit a variety of crimes including, *e.g.*, opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' names

to obtain medical services, using Class Members' information to obtain government benefits, filing fraudulent tax returns and insurance claims using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

9. There has been no assurance offered by Zeroed-In that all personal data or copies of data have been recovered or destroyed, or that Defendant has adequately enhanced its data security practices sufficient to avoid a similar breach of its network in the future.

10. Therefore, Plaintiffs and Class Members have suffered and are at an imminent, immediate, and continuing increased risk of suffering, ascertainable losses in the form of harm from identity theft and other fraudulent misuse of their Private Information, the loss of the benefit of their bargain, out-of-pocket expenses incurred to remedy or mitigate the effects of the Data Breach, and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach.

11. Plaintiffs brings this class action lawsuit to address Zeroed-In's inadequate safeguarding of Class Members' Private Information that it collected and maintained, and its failure to provide timely and adequate notice to Plaintiffs and Class Members of the types of information that were accessed, and that such information was subject to unauthorized access by cybercriminals.

12. The potential for improper disclosure and theft of Plaintiffs' and Class Members' Private Information was a known risk to Zeroed-In, and thus Zeroed-In was on notice that failing to take necessary steps to secure the Private Information left it vulnerable to an attack.

13. Upon information and belief, Zeroed-In failed to properly monitor and implement proper security practices with regard to the computer network that housed the Private Information. Had Zeroed-In properly monitored its networks, it would have discovered the Breach sooner.

14. Plaintiffs' and Class Members' identities are now at risk because of Zeroed-In's negligent conduct as the Private Information that Zeroed-In collected and maintained is now in the hands of data thieves and other unauthorized third parties.

15. Plaintiffs seek to remedy this harm on behalf of themselves and all similarly situated individuals whose Private Information was accessed and/or compromised during the Data Breach.

16. Accordingly, Plaintiffs, on behalf of themselves and the Class, assert claims for negligence, negligence *per se*, breach of third-party beneficiary contract, breach of implied contract, unjust enrichment, and declaratory judgment.

II. PARTIES

17. Plaintiff Nicholas Pierce is, and at all times mentioned herein was, an individual citizen of the State of New York.

18. Plaintiff Misty Hunter is, and at all times mentioned herein was, an individual citizen of the State of Alabama.

19. Defendant Zeroed-In is a limited liability company organized under the laws of the State of Florida. Zeroed-In maintains its principal place of business at 11037 Harbor Yacht Ct., #201, Fort Myers, Florida 33908, with its mailing address maintained at 8595 College Parkway, Suite 350, Fort Myers, Florida 33919.

III. JURISDICTION AND VENUE

20. The Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. Upon information and belief, the number of class members is over 100, many of whom have different citizenship from Zeroed-In. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

21. This Court has jurisdiction over Zeroed-In because Zeroed-In's principal place of business is located in this District. Christopher Moore, who is identified as the CEO and "Manager" of Zeroed-In on Zeroed-In's most recent annual report filed with the Florida Secretary of State on January 18, 2023, also has an address within this District: 11037 Harbor Yacht Ct., #201, Fort Myers, Florida 33908.

22. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events giving rise to this action occurred in this District and Zeroed-In has harmed Class Members residing in this District.

IV. FACTUAL ALLEGATIONS

A. Zeroed-In's Business and Collection of Plaintiffs' and Class Members' Private Information Zeroed-In

23. Zeroed-In is a data and technology consulting firm that provides workforce analytics solutions to its corporate clients. Zeroed-In specializes in data management, data visualization, human resources, and people analytics. Founded in 2004, Zeroed-In employs more than 2,500 people and generates approximately $5.2 million in annual revenue.

24. As a condition of receiving HR data analytics services, Zeroed-In requires that its clients and its clients' employees entrust it with highly sensitive personal information. In the ordinary course of receiving service from Zeroed-In, Plaintiffs and Class Members were required

to provide their Private Information to Defendant, through their employer (one of Defendant's clients).

25. In its Privacy Policy, Zeroed-In promises its clients and clients' employees that it is "committed to protecting the privacy of your information" and that it "employ[s] robust security measures to protect against the loss, misuse and alternation of the personal information under our control."[1] Zeroed-In also maintains that "[k]eeping your personal information secure is our first priority." *Id.*

26. Thus, due to the highly sensitive and personal nature of the information Zeroed-In acquires and stores with respect to its clients' employees, Zeroed-In, upon information and belief, promises to, among other things: keep employees' Private Information private; comply with industry standards related to data security and the maintenance of employees' Private Information; inform employees of its legal duties relating to data security and comply with all federal and state laws protecting employees' Private Information; only use and release employees' Private Information for reasons that relate to the services it provides; and provide adequate notice to employees if their Private Information is disclosed without authorization.

27. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' Private Information, Zeroed-In assumed legal and equitable duties it owed to them and knew or should have known that it was responsible for protecting Plaintiffs' and Class Members' Private Information from unauthorized disclosure and exfiltration.

28. Plaintiffs and Class Members relied on Zeroed-In to keep their Private Information confidential and securely maintained and to only make authorized disclosures of this Information, which Defendant ultimately failed to do.

[1] See https://www.zeroedin.com/privacy-policy/ (last visited Nov. 29, 2023).

B. The Data Breach and Defendant's Inadequate Notice to Plaintiffs and Class Members

29. According to Defendant's Notice, it learned of unauthorized access to its computer systems on August 8, 2023, with such unauthorized access having taken place between August 7, 2023, and August 8, 2023.

30. Through the Data Breach, the unauthorized cybercriminal(s) accessed a cache of highly sensitive Private Information, including name, date of birth, and Social Security numbers.

31. On or about November 27, 2023, roughly four months after Zeroed-In learned that the Class's Private Information was first accessed by cybercriminals, Zeroed-In finally began to notify its clients' employees' that its investigation determined that their Private Information was impacted.

32. Zeroed-In had obligations created by contract, industry standards, common law, and representations made to Plaintiffs and Class Members to keep Plaintiffs' and Class Members' Private Information confidential and to protect it from unauthorized access and disclosure.

33. Plaintiffs and Class Members provided their Private Information to Zeroed-In with the reasonable expectation and mutual understanding that Zeroed-In would comply with its obligations to keep such Information confidential and secure from unauthorized access and to provide timely notice of any security breaches.

34. Zeroed-In's data security obligations were particularly important given the substantial increase in cyberattacks in recent years.

35. Zeroed-In knew or should have known that its electronic records would be targeted by cybercriminals.

C. Zeroed-In Failed to Comply with FTC Guidelines

36. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision making. Indeed, the FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

37. In October 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cybersecurity guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep, properly dispose of personal information that is no longer needed, encrypt information stored on computer networks, understand their network's vulnerabilities, and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs, monitor all incoming traffic for activity indicating someone is attempting to hack into the system, watch for large amounts of data being transmitted from the system, and have a response plan ready in the event of a breach.

38. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction, limit access to sensitive data, require complex passwords to be used on networks, use industry-tested methods for security, monitor the network for suspicious activity, and verify that third-party service providers have implemented reasonable security measures.

39. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data by treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by the FTCA. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

40. As evidenced by the Data Breach, Zeroed-In failed to properly implement basic data security practices. Zeroed-In's failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiffs' and Class Members' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA.

41. Zeroed-In was at all times fully aware of its obligation to protect the Private Information of its clients' employees yet failed to comply with such obligations. Defendant was also aware of the significant repercussions that would result from its failure to do so.

D. Zeroed-In Failed to Comply with Industry Standards

42. As noted above, experts studying cybersecurity routinely identify businesses as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

43. Some industry best practices that should be implemented by businesses dealing with sensitive PII like Zeroed-In include but are not limited to: educating all employees, strong password requirements, multilayer security including firewalls, anti-virus and anti-malware software, encryption, multi-factor authentication, backing up data, and limiting which employees can access sensitive data. As evidenced by the Data Breach, Defendant failed to follow some or all of these industry best practices.

44. Other best cybersecurity practices that are standard in the industry include: installing appropriate malware detection software; monitoring and limiting network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protecting physical security systems; and training staff regarding these points. As evidenced by the Data Breach, Defendant failed to follow these cybersecurity best practices.

45. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

46. Defendant failed to comply with these accepted standards, thereby permitting the Data Breach to occur.

E. Zeroed-In Breached its Duty to Safeguard Plaintiffs' and Class Members' Private Information

47. In addition to its obligations under federal and state laws, Zeroed-In owed a duty to Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Zeroed-In owed a duty to Plaintiffs and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems, networks, and protocols adequately protected the Private Information of Class Members

48. Zeroed-In breached its obligations to Plaintiffs and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data. Zeroed-In's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system that would reduce the risk of data breaches and cyberattacks;

b. Failing to adequately protect employees' Private Information;

c. Failing to properly monitor its own data security systems for existing intrusions;

d. Failing to sufficiently train its employees regarding the proper handling of its clients' employees' Private Information;

e. Failing to fully comply with FTC guidelines for cybersecurity in violation of the FTCA; and

f. Otherwise breaching its duties and obligations to protect Plaintiffs' and Class Members' Private Information.

49. Zeroed-In negligently and unlawfully failed to safeguard Plaintiffs' and Class Members' Private Information by allowing cyberthieves to access its computer network and systems which contained unsecured and unencrypted Private Information.

50. Had Zeroed-In remedied the deficiencies in its information storage and security systems, followed industry guidelines, and adopted security measures recommended by experts in the field, it could have prevented intrusion into its information storage and security systems and, ultimately, the theft of Plaintiffs' and Class Members' confidential Private Information.

51. Accordingly, Plaintiffs' and Class Members' lives were severely disrupted. What's more, they have been harmed as a result of the Data Breach and now face an increased risk of

future harm that includes, but is not limited to, fraud and identity theft. Plaintiffs and Class Members also lost the benefit of the bargain they made with Zeroed-In

F. Zeroed-In Should Have Known that Cybercriminals Target PII to Carry Out Fraud and Identity Theft

52. The FTC hosted a workshop to discuss "informational injuries," which are injuries that consumers like Plaintiffs and Class Members suffer from privacy and security incidents such as data breaches or unauthorized disclosure of data.[2] Exposure of highly sensitive personal information that a consumer wishes to keep private may cause harm to the consumer, such as the ability to obtain or keep employment. Consumers' loss of trust in e-commerce also deprives them of the benefits provided by the full range of goods and services available which can have negative impacts on daily life.

53. Any victim of a data breach is exposed to serious ramifications regardless of the nature of the data that was breached. Indeed, the reason why criminals steal information is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims or to take over victims' identities in order to engage in illegal financial transactions under the victims' names.

54. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity or to otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security

[2] *FTC Information Injury Workshop, BE and BCP Staff Perspective*, Federal Trade Commission, (October 2018), *available at* https://www.ftc.gov/system/files/documents/reports/ftc-informational-injury-workshop-be-bcp-staff-perspective/informational_injury_workshop_staff_report_-_oct_2018_0.pdf (last visited on Nov. 29, 2023).

number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

55. In fact, as technology advances, computer programs may scan the Internet with a wider scope to create a mosaic of information that may be used to link compromised information to an individual in ways that were not previously possible. This is known as the "mosaic effect." Names and dates of birth, combined with contact information like telephone numbers and email addresses, are very valuable to hackers and identity thieves as it allows them to access users' other accounts.

56. Thus, even if certain information was not purportedly involved in the Data Breach, the unauthorized parties could use Plaintiffs' and Class Members' Private Information to access accounts, including, but not limited to, email accounts and financial accounts, to engage in a wide variety of fraudulent activity against Plaintiffs and Class Members.

57. One such example of this is the development of "Fullz" packages.

58. Cybercriminals can cross-reference two sources of the Private Information compromised in the Data Breach to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

59. The development of "Fullz" packages means that the stolen Private Information from the Data Breach can easily be used to link and identify it to Plaintiffs' and the proposed Class's phone numbers, email addresses, and other sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card or financial account numbers may not be included in the Private Information stolen in the Data Breach, criminals can easily

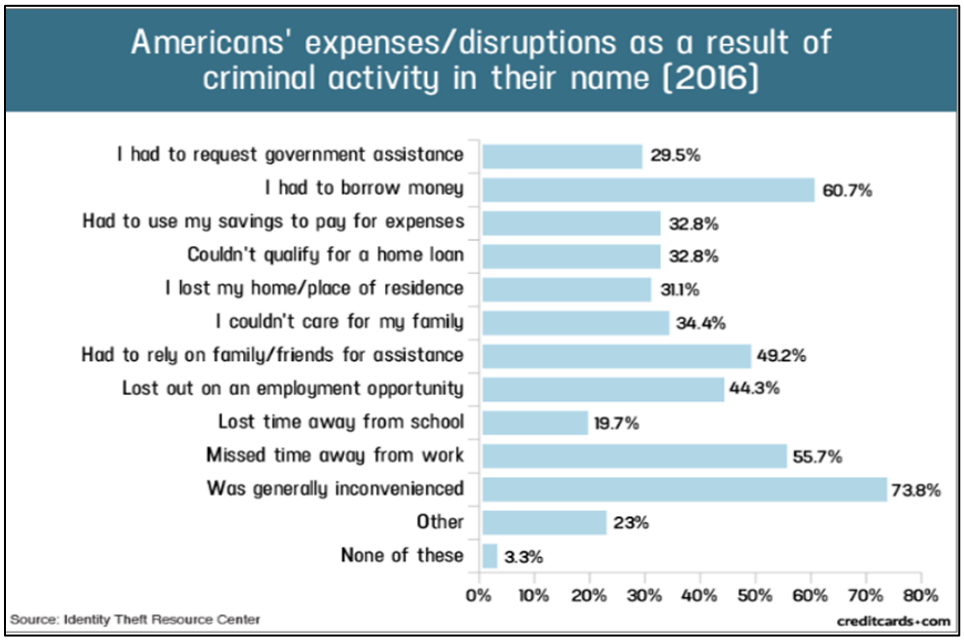
create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiffs and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiffs and other Class Members' stolen Private Information is being misused, and that such misuse is fairly traceable to the Data Breach.

60. For these reasons, the FTC recommends that identity theft victims take several time-consuming steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert on their account (and an extended fraud alert that lasts for 7 years if someone steals the victim's identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a freeze on their credit, and correcting their credit reports.[3] However, these steps do not guarantee protection from identity theft but can only mitigate identity theft's long-lasting negative impacts.

61. Identity thieves can also use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, bank fraud, to obtain a driver's license or official identification card in the victim's name but with the thief's picture, to obtain government benefits, or to file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house in the victim's name, receive medical services in the victim's name, and even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

[3] *See IdentityTheft.gov*, Federal Trade Commission, *available at* https://www.identitytheft.gov/Steps (last visited Nov. 29, 2023).

62. In fact, a study by the Identity Theft Resource Center[4] shows the multitude of harms caused by fraudulent use of PII:



63. The ramifications of Zeroed-In's failure to keep its client's employees' Private Information secure are long-lasting and severe. Once it is stolen, fraudulent use of such and damage to victims may continue for years.

64. Here, Social Security numbers were compromised. The value of PII is axiomatic. The value of "big data" in corporate America is astronomical. The fact that identity thieves attempt to steal identities notwithstanding possible heavy prison sentences illustrates beyond a doubt that the Private Information compromised here has considerable market value.

65. It must also be noted that there may be a substantial time lag between when harm occurs and when it is discovered, and also between when PII is stolen and when it is misused.

[4] Steele, Jason, *Credit Card and ID Theft Statistics*, CreditCards.com (October 23, 2017), *available at* https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276/ (last visited on Nov. 29 ,2023).

According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:[5]

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

66. PII is such a valuable commodity to identity thieves that once it has been compromised, criminals often trade the information on the dark web for years.

67. As a result, Plaintiffs and Class Members are at an increased risk of fraud and identity theft, including medical identity theft, for many years into the future. Thus, Plaintiffs and Class Members have no choice but to vigilantly monitor their accounts for many years to come.

G. Plaintiffs' and Class Members' Damages

Plaintiff Nicholas Pierce's Experience

68. When Plaintiff became employed by one of Defendant's clients, Defendant required substantial amounts of his Private Information, including Social Security numbers.

69. On or about November 27, 2023, Plaintiff Pierce received a letter entitled "Notice of Security Incident" which told him that his Private Information had been involved in the Data Breach. The notice letter informed him that the Private Information stolen included his "name, date of birth, and Social Security number."

[5] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO (June 2007), *available at* https://www.gao.gov/assets/270/262904.html (last visited Nov. 29, 2023).

70. The notice letter only offered Plaintiff one year of credit monitoring services. One year of credit monitoring is insufficient given that Plaintiff will now experience a lifetime of increased risk of identity theft, including but not limited to, potential medical fraud.

71. Plaintiff suffered actual injury in the form of time spent dealing with the Data Breach and the increased risk of fraud resulting from the Data Breach and/or monitoring his accounts for fraud.

72. Plaintiff would not have provided his Private Information to Defendant had Defendant timely disclosed that its systems lacked adequate computer and data security practices to safeguard its clients' employees' personal information from theft, and that those systems were subject to a data breach.

73. Plaintiff suffered actual injury in the form of having his PII compromised and/or stolen as a result of the Data Breach.

74. Plaintiff suffered actual injury in the form of damages to and diminution in the value of his personal information – a form of intangible property that Plaintiff entrusted to Defendant for the purpose of receiving services from Defendant and which was compromised in, and as a result of, the Data Breach.

75. Plaintiff suffered imminent and impending injury arising from the substantially increased risk of future fraud, identity theft, and misuse posed by his Private Information being placed in the hands of criminals.

76. Plaintiff has a continuing interest in ensuring that his PII, which remains in the possession of Defendant, is protected and safeguarded from future breaches.

77. As a result of the Data Breach, Plaintiff made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, reviewing

financial accounts for any indications of actual or attempted identity theft or fraud, and researching the credit monitoring offered by Defendant. Plaintiff has spent several hours dealing with the Data Breach – valuable time he otherwise would have spent on other activities.

78. As a result of the Data Breach, Plaintiff has suffered anxiety as a result of the release of his PII, which he believed would be protected from unauthorized access and disclosure. These feelings include anxiety about unauthorized parties viewing, selling, and/or using his PII for purposes of committing cyber and other crimes against him including, but not limited to, fraud and identity theft. Plaintiff is very concerned about this increased, substantial, and continuing risk, as well as the consequences that identity theft and fraud resulting from the Data Breach would have on his life.

79. Plaintiff also suffered actual injury from having his Private Information compromised as a result of the Data Breach in the form of (a) damage to and diminution in the value of his PII, a form of property that Defendant obtained, directly or indirectly, from Plaintiff; (b) violation of his privacy rights; and (c) present, imminent, and impending injury arising from the increased risk of identity theft, and fraud he now faces.

80. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the many harms caused by the Data Breach.

Plaintiff Misty Hunter's Experience

81. When Plaintiff became employed by one of Defendant's clients, Defendant required substantial amounts of her Private Information, including Social Security numbers.

82. On or about November 27, 2023, Plaintiff Hunter received a letter entitled "Notice of Security Incident" which told her that her Private Information had been involved in the Data

Breach. The notice letter informed her that the Private Information stolen included her "name, date of birth, and Social Security number."

83. The notice letter only offered Plaintiff one year of credit monitoring services. One year of credit monitoring is insufficient given that Plaintiff will now experience a lifetime of increased risk of identity theft, including but not limited to, potential medical fraud.

84. In fact, Plaintiff Hunter recently noticed that funds from her bank account had been removed without her knowledge or authorization.

85. Plaintiff also suffered actual injury in the form of time spent dealing with the Data Breach and the increased risk of fraud resulting from the Data Breach and monitoring her other accounts for similar fraud.

86. Plaintiff would not have provided her Private Information to Defendant had Defendant timely disclosed that its systems lacked adequate computer and data security practices to safeguard its clients' employees' personal information from theft, and that those systems were subject to a data breach.

87. Plaintiff suffered actual injury in the form of having her PII compromised and/or stolen as a result of the Data Breach.

88. Plaintiff suffered actual injury in the form of damages to and diminution in the value of her personal information – a form of intangible property that Plaintiff entrusted to Defendant for the purpose of receiving services from Defendant and which was compromised in, and as a result of, the Data Breach.

89. Plaintiff suffered imminent and impending injury arising from the substantially increased risk of future fraud, identity theft, and misuse posed by her Private Information being placed in the hands of criminals.

90. Plaintiff has a continuing interest in ensuring that her PII, which remains in the possession of Defendant, is protected and safeguarded from future breaches.

91. As a result of the Data Breach, Plaintiff made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, reviewing financial accounts for any indications of actual or attempted identity theft or fraud, and researching the credit monitoring offered by Defendant. Plaintiff has spent several hours dealing with the Data Breach – valuable time she otherwise would have spent on other activities.

92. As a result of the Data Breach, Plaintiff has suffered anxiety as a result of the release of her PII, which she believed would be protected from unauthorized access and disclosure. These feelings include anxiety about unauthorized parties viewing, selling, and/or using her PII for purposes of committing cyber and other crimes against her including, but not limited to, fraud and identity theft in addition to the fraud she has already experienced. Plaintiff is very concerned about this increased, substantial, and continuing risk, as well as the consequences that identity theft and fraud resulting from the Data Breach will have on her life.

93. Plaintiff also suffered actual injury from having her Private Information compromised as a result of the Data Breach in the form of (a) damage to and diminution in the value of her PII, a form of property that Defendant obtained, directly or indirectly, from Plaintiff; (b) violation of her privacy rights; and (c) present, imminent, and impending injury arising from the increased risk of identity theft, and fraud she now faces.

94. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the many harms caused by the Data Breach.

95. In sum, Plaintiffs and Class Members have been damaged by the compromise of their Private Information in the Data Breach.

96. Plaintiffs and Class Members entrusted their Private Information to Defendant in order to benefit from Defendant's services.

97. Their Private Information was subsequently compromised as a direct and proximate result of the Data Breach, which Data Breach resulted from Defendant's inadequate data security practices.

98. As a direct and proximate result of Zeroed-In's actions and omissions, Plaintiffs and Class Members have been harmed and are at an imminent, immediate, and continuing increased risk of harm, including but not limited to, having medical services billed in their names, loans opened in their names, tax returns filed in their names, utility bills opened in their names, credit card accounts opened in their names, and other forms of identity theft.

99. Further, and as set forth above, as a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have also been forced to take the time and effort to mitigate the actual and potential impact of the data breach on their everyday lives, including placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

100. Plaintiffs and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

101. Plaintiffs and Class Members also face a substantial risk of being targeted in future phishing, data intrusion, and other illegal schemes through the misuse of their Private Information,

since potential fraudsters will likely use such Private Information to carry out such targeted schemes against Plaintiffs and Class Members.

102. The Private Information maintained by and stolen from Defendant's systems, combined with publicly available information, allows nefarious actors to assemble a detailed mosaic of Plaintiffs and Class Members, which can also be used to carry out targeted fraudulent schemes against Plaintiffs and Class Members.

103. Additionally, Plaintiffs and Class Members also suffered a loss of value of their PII when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases. An active and robust legitimate marketplace for Private Information also exists. In 2019, the data brokering industry was worth roughly $200 billion.[6] In fact, consumers who agree to provide their web browsing history to the Nielsen Corporation can in turn receive up to $50 a year.[7]

104. As a result of the Data Breach, Plaintiffs' and Class Members' Private Information, which has an inherent market value in both legitimate and illegal markets, has been harmed and diminished due to its acquisition by cybercriminals. This transfer of valuable information happened with no consideration paid to Plaintiffs or Class Members for their property, resulting in an economic loss. Moreover, the Private Information is apparently readily available to others, and the rarity of the Private Information has been destroyed because it is no longer only held by Plaintiffs and the Class Members, and because that data no longer necessarily correlates only with activities undertaken by Plaintiffs and the Class Members, thereby causing additional loss of value.

---

[6] *See* https://thequantumrecord.com/blog/data-brokers-profit-from-our-data/#:~:text=The%20business%20of%20data%20brokering,annual%20revenue%20of%20%24200%20billion. (last visited on Nov. 29, 2023).

[7] *Frequently Asked Questions*, Nielsen Computer & Mobile Panel, https://computermobilepanel.nielsen.com/ui/US/en/faqen.html (last visited on Nov. 29 ,2023).

105. Finally, Plaintiffs and Class Members have suffered or will suffer actual injury as a direct and proximate result of the Data Breach in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach.

106. Moreover, Plaintiffs and Class Members have an interest in ensuring that their Private Information, which is believed to still be in the possession of Zeroed-In, is protected from future breaches by the implementation of more adequate data security measures and safeguards, including but not limited to, ensuring that the storage of data or documents containing highly sensitive personal information of its clients' employees is not accessible online, that access to such data is password-protected, and that such data is properly encrypted.

107. As a direct and proximate result of Zeroed-In's actions and inactions, Plaintiffs and Class Members have suffered a loss of privacy and have suffered cognizable harm, including an imminent and substantial future risk of harm, in the forms set forth above.

V. CLASS ACTION ALLEGATIONS

108. Plaintiffs bring this action individually and on behalf of all other persons similarly situated, pursuant to Federal Rule of Civil Procedure 23(a), 23(b)(1), 23(b)(2), and 23(b)(3).

109. Specifically, Plaintiffs propose the following Nationwide Class, (referred to herein as the "Class"), subject to amendment as appropriate:

> **Nationwide Class**
>
> All individuals in the United States who had Private Information accessed and/or acquired as a result of the Data Breach, including all who were sent a notice of the Data Breach.

110. Excluded from the Class are Defendant and its parents or subsidiaries, any entities in which it has a controlling interest, as well as its officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns. Also excluded is any Judge to whom this case is assigned as well as their judicial staff and immediate family members.

111. Plaintiffs reserve the right to modify or amend the definitions of the proposed Nationwide Class and/or add subclasses before the Court determines whether certification is appropriate.

112. The proposed Class meets the criteria for certification under Fed. R. Civ. P. 23(a), (b)(2), and (b)(3).

113. Numerosity. The Class Members are so numerous that joinder of all members is impracticable. Though the exact number and identities of Class Members are unknown at this time, based on information and belief, the Class consists of 1,977,486 affected individuals of Zeroed-In whose data was compromised in the Data Breach.[8] The identities of Class Members are ascertainable through Zeroed-In's records, Class Members' records, publication notice, self-identification, and other means.

114. Commonality. There are questions of law and fact common to the Class which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Zeroed-In engaged in the conduct alleged herein;

b. Whether Zeroed-In's conduct violated the FTCA;

c. When Zeroed-In learned of the Data Breach;

d. Whether Zeroed-In's response to the Data Breach was adequate;

e. Whether Zeroed-In unlawfully lost or disclosed Plaintiffs' and Class Members' Private Information;

[8] See https://apps.web.maine.gov/online/aeviewer/ME/40/b3993ddd-2443-4645-ae45-f36dc7686236.shtml / (last visited December 4, 2023).

f. Whether Zeroed-In failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the Private Information compromised in the Data Breach;

g. Whether Zeroed-In's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

h. Whether Zeroed-In's data security systems prior to and during the Data Breach were consistent with industry standards;

i. Whether Zeroed-In owed a duty to Class Members to safeguard their Private Information;

j. Whether Zeroed-In breached its duty to Class Members to safeguard their Private Information;

k. Whether hackers obtained Class Members' Private Information via the Data Breach;

l. Whether Zeroed-In had a legal duty to provide timely and accurate notice of the Data Breach to Plaintiffs and the Class Members;

m. Whether Zeroed-In breached its duty to provide timely and accurate notice of the Data Breach to Plaintiffs and Class Members;

n. Whether Zeroed-In knew or should have known that its data security systems and monitoring processes were deficient;

o. What damages Plaintiffs and Class Members suffered as a result of Zeroed-In's misconduct;

p. Whether Zeroed-In's conduct was negligent;

q. Whether Zeroed-In's conduct was *per se* negligent;

r. Whether Zeroed-In's was unjustly enriched;

s. Whether Plaintiffs and Class Members are entitled to actual and/or statutory damages;

t. Whether Plaintiffs and Class Members are entitled to additional credit or identity monitoring and monetary relief; and

u. Whether Plaintiffs and Class Members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

115. Typicality. Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' Private Information, like that of every other Class Member, was compromised in the Data Breach. Plaintiffs' claims are typical of those of the other Class Members because, *inter alia*, all Class Members were injured through the common misconduct of Zeroed-In. Plaintiffs are advancing the same claims and legal theories on behalf of themselves and all other Class Members, and there are no defenses that are unique to Plaintiffs. The claims of Plaintiffs and those of Class Members arise from the same operative facts and are based on the same legal theories.

116. Adequacy of Representation. Plaintiffs will fairly and adequately represent and protect the interests of Class Members. Plaintiffs' counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

117. Predominance. Zeroed-In has engaged in a common course of conduct toward Plaintiffs and Class Members in that all of Plaintiffs' and Class Members' data was stored on the same computer systems and unlawfully accessed and exfiltrated in the same way. The common issues arising from Zeroed-In's conduct affecting Class Members set out above predominate over

any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

118. Superiority. A Class action is superior to other available methods for the fair and efficient adjudication of this controversy and no unusual difficulties are likely to be encountered in the management of this class action. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a Class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Zeroed-In. In contrast, conducting this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

119. Class certification is also appropriate under Fed. R. Civ. P. 23(b)(2). Zeroed-In has acted and/or refused to act on grounds generally applicable to the Class such that final injunctive relief and/or corresponding declaratory relief is appropriate as to the Class as a whole.

120. Finally, all members of the proposed Class are readily ascertainable. Zeroed-In has access to the names and addresses and/or email addresses of Class Members affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Zeroed-In.

CLAIMS FOR RELIEF

COUNT I
NEGLIGENCE
(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS)

121. Plaintiffs restate and reallege the allegations in paragraphs 1 to 121 as if fully set forth herein.

122. Zeroed-In knowingly collected, came into possession of, and maintained Plaintiffs' and Class Members' Private Information, and had a duty to exercise reasonable care in safeguarding, securing, and protecting such Information from being disclosed, compromised, lost, stolen, and misused by unauthorized parties.

123. Zeroed-In's duty also included a responsibility to implement processes by which it could detect and analyze a breach of its security systems quickly and to give prompt notice to those affected in the case of a cyberattack.

124. Zeroed-In knew or should have known of the risks inherent in collecting the Private Information of Plaintiffs and Class Members and the importance of adequate security. Zeroed-In was on notice because, on information and belief, it knew or should have known that it would be an attractive target for cyberattacks.

125. Zeroed-In owed a duty of care to Plaintiffs and Class Members whose Private Information was entrusted to it. Zeroed-In's duties included, but were not limited to, the following:

a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting Private Information in its possession;

b. To protect employees' Private Information using reasonable and adequate security procedures and systems compliant with industry standards;

c. To have procedures in place to prevent the loss or unauthorized dissemination of Private Information in its possession;

d. To employ reasonable security measures and otherwise protect the Private Information of Plaintiffs and Class Members pursuant to the FTCA;

e. To implement processes to quickly detect a data breach and to timely act on warnings about data breaches; and

f. To promptly notify Plaintiffs and Class Members of the Data Breach, and to precisely disclose the type(s) of information compromised.

126. Zeroed-In's duty to employ reasonable data security measures arose, in part, under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

127. Zeroed-In's duty also arose because Defendant was bound by industry standards to protect its clients' employees' confidential Private Information.

128. Plaintiffs and Class Members were foreseeable victims of any inadequate security practices on the part of Defendant, and Zeroed-In owed them a duty of care to not subject them to an unreasonable risk of harm.

129. Zeroed-In, through its actions and/or omissions, unlawfully breached its duty to Plaintiffs and Class Members by failing to exercise reasonable care in protecting and safeguarding Plaintiffs' and Class Members' Private Information within Zeroed-In's possession.

130. Zeroed-In, by its actions and/or omissions, breached its duty of care by failing to provide, or acting with reckless disregard for, fair, reasonable, or adequate computer systems and data security practices to safeguard the Private Information of Plaintiffs and Class Members.

131. Zeroed-In, by its actions and/or omissions, breached its duty of care by failing to promptly identify the Data Breach and then failing to provide prompt notice of the Data Breach to the persons whose Private Information was compromised.

132. Zeroed-In breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;

b. Failing to adequately monitor the security of its networks and systems;

c. Failing to periodically ensure that its email system maintained reasonable data security safeguards;

d. Allowing unauthorized access to Class Members' Private Information;

e. Failing to comply with the FTCA;

f. Failing to detect in a timely manner that Class Members' Private Information had been compromised; and

g. Failing to timely notify Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

133. Zeroed-In acted with reckless disregard for the rights of Plaintiffs and Class Members by failing to provide prompt and adequate individual notice of the Data Breach such that Plaintiffs and Class Members could take measures to protect themselves from damages caused by the fraudulent use of the Private Information compromised in the Data Breach.

134. Zeroed-In had a special relationship with Plaintiffs and Class Members. Plaintiffs' and Class Members' willingness to entrust Zeroed-In with their Private Information was predicated

on the understanding that Zeroed-In would take adequate security precautions. Moreover, only Zeroed-In had the ability to protect its systems (and the Private Information that it stored on them) from attack.

135. Zeroed-In's breach of duties owed to Plaintiffs and Class Members caused Plaintiffs' and Class Members' Private Information to be compromised and exfiltrated and alleged herein.

136. As a result of Zeroed-In's ongoing failure to notify Plaintiffs and Class Members regarding exactly what Private Information has been compromised, Plaintiffs and Class Members have been unable to take the necessary precautions to prevent future fraud and mitigate damages.

137. Zeroed-In's breaches of duty also caused a substantial, imminent risk to Plaintiffs and Class Members of identity theft, loss of control over their Private Information, and/or loss of time and money to monitor their accounts for fraud.

138. As a result of Zeroed-In's negligence in breach of its duties owed to Plaintiffs and Class Members, Plaintiffs and Class Members are in danger of imminent harm in that their Private Information, which is still in the possession of third parties, will be used for fraudulent purposes.

139. Zeroed-In also had independent duties under state laws that required it to reasonably safeguard Plaintiffs' and Class Members' Private Information and promptly notify them about the Data Breach.

140. As a direct and proximate result of Zeroed-In's negligent conduct, Plaintiffs and Class Members have suffered damages as alleged herein and are at imminent risk of further harm.

141. The injury and harm that Plaintiffs and Class Members suffered was reasonably foreseeable.

142. Plaintiffs and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

143. In addition to monetary relief, Plaintiffs and Class Members are also entitled to injunctive relief requiring Zeroed-In to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members.

COUNT II
NEGLIGENCE *PER SE*
(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS)

144. Plaintiffs restate and reallege the allegations in paragraphs 1 to 121 as if fully set forth herein.

145. Pursuant to Section 5 of the FTCA, Zeroed-In had a duty to provide fair and adequate computer systems and data security to safeguard the Private Information of Plaintiffs and Class Members.

146. Zeroed-In breached its duties to Plaintiffs and Class Members under the FTCA by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Private Information.

147. Specifically, Zeroed-In breached its duties by failing to employ industry-standard cybersecurity measures in order to comply with the FTCA, including but not limited to proper segregation, access controls, password protection, encryption, intrusion detection, secure destruction of unnecessary data, and penetration testing.

148. The FTCA prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice of failing to use reasonable measures to protect PII (such as the Private Information compromised in the Data Breach). The FTC rulings

and publications described above, together with the industry-standard cybersecurity measures set forth herein, form part of the basis of Zeroed-In's duty in this regard.

149. Zeroed-In also violated the FTCA by failing to use reasonable measures to protect the Private Information of Plaintiffs and the Class and by not complying with applicable industry standards, as described herein.

150. It was reasonably foreseeable, particularly given the growing number of data breaches of Private Information, that the failure to reasonably protect and secure Plaintiffs' and Class Members' Private Information in compliance with applicable laws would result in an unauthorized third-party gaining access to Zeroed-In's networks, databases, and computers that stored Plaintiffs' and Class Members' unencrypted Private Information.

151. Plaintiffs and Class Members are within the class of persons that the FTCA is intended to protect and Zeroed-In's failure to comply with both constitutes negligence *per se*.

152. Plaintiffs' and Class Members' Private Information constitutes personal property that was stolen due to Zeroed-In's negligence, resulting in harm, injury, and damages to Plaintiffs and Class Members.

153. As a direct and proximate result of Zeroed-In's negligence *per se*, Plaintiffs and the Class have suffered, and continue to suffer, injuries and damages arising from the unauthorized access of their Private Information, including but not limited to damages for the lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives.

154. As a direct and proximate result of Zeroed-In's negligent conduct, Plaintiffs and Class Members have suffered injury and are entitled to compensatory and consequential damages in an amount to be proven at trial.

155. In addition to monetary relief, Plaintiffs and Class Members are also entitled to injunctive relief requiring Zeroed-In to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members.

COUNT III
BREACH OF THIRD-PARTY BENEFICIARY CONTRACT
(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS)

156. Plaintiffs restate and reallege the allegations in paragraphs 1 to 121 as if fully set forth herein.

157. Defendant entered into contracts, written or implied, with its clients to perform services that include, but are not limited to, providing HR data analytics services to said clients. Upon information and belief, these contracts are virtually identical between and among Defendant and its clients around the country whose employees, including Plaintiffs and Class Members, were affected by the Data Breach.

158. In exchange, Defendant agreed, in part, to implement adequate security measures to safeguard the PII of Plaintiffs and the Class.

159. These contracts were made expressly for the benefit of Plaintiffs and the Class, as Plaintiffs and Class Members were the intended third-party beneficiaries of the contracts entered into between Defendant and its clients. Defendant knew that if it were to breach these contracts with its clients, the clients' employees—Plaintiffs and Class Members—would be harmed.

160. Defendant breached the contracts it entered into with its clients by, among other things, failing to (i) use reasonable data security measures, (ii) implement adequate protocols and employee training sufficient to protect Plaintiffs' Private Information from unauthorized

disclosure to third parties, and (iii) promptly and adequately detecting the Data Breach and notifying Plaintiffs and Class Members thereof.

161. Plaintiffs and the Class were harmed by Defendant's breach of its contracts with its clients, as such breach is alleged herein, and are entitled to the losses and damages they have sustained as a direct and proximate result thereof.

162. Plaintiffs and Class Members are also entitled to their costs and attorney's fees incurred in this action.

COUNT IV
BREACH OF IMPLIED CONTRACT
(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS)

163. Plaintiffs restate and reallege the allegations in paragraphs 1 to 121 as if fully set forth herein.

164. This Count is pleaded in the alternative to Count III above.

165. Zeroed-In provides HR and data analytics services to its corporate clients and their employees—Plaintiffs and Class Members. Plaintiffs and Class Members formed an implied contract with Defendant regarding the provision of those services through their collective conduct, including by Plaintiffs and Class Members entrusting their valuable Private Information to Defendant in exchange for such services.

166. Through Defendant's provision of services to Plaintiffs and Class Members and their respective employers, it knew or should have known that it must protect Plaintiffs' and Class Members' confidential Private Information in accordance with its policies, practices, and applicable law.

167. As consideration, Plaintiffs and Class Members paid money to Zeroed-In and/or turned over valuable Private Information to Zeroed-In. Accordingly, Plaintiffs and Class Members bargained with Zeroed-In to securely maintain and store their Private Information.

168. Zeroed-In accepted payment and/or possession of Plaintiffs' and Class Members' Private Information for the purpose of providing services to Plaintiffs and Class Members.

169. In providing their valuable Private Information to Defendant in exchange for Defendant's services, Plaintiffs and Class Members intended and understood that Zeroed-In would adequately safeguard the Private Information as part of those services.

170. Defendant's implied promises to Plaintiffs and Class Members include, but are not limited to, (1) taking steps to ensure that anyone who is granted access to Private Information also protect the confidentiality of that data; (2) taking steps to ensure that the Private Information that is placed in the control of its employees is restricted and limited to achieve an authorized business purpose; (3) restricting access to qualified and trained employees and/or agents; (4) designing and implementing appropriate retention policies to protect the Private Information against criminal data breaches; (5) applying or requiring proper encryption; (6) implementing multifactor authentication for access; and (7) taking other steps to protect against foreseeable data breaches.

171. Plaintiffs and Class Members would not have entrusted their Private Information to Zeroed-In in the absence of such an implied contract.

172. Had Zeroed-In disclosed to Plaintiffs and the Class that it did not have adequate computer systems and security practices to secure sensitive data, Plaintiffs and Class Members would not have provided their Private Information to Zeroed-In

173. Zeroed-In recognized (or should have recognized) that Plaintiffs' and Class Member's Private Information is highly sensitive and must be protected, and that this protection was of material importance as part of the bargain with Plaintiffs and the other Class Members.

174. Zeroed-In violated these implied contracts by failing to employ reasonable and adequate security measures to secure Plaintiffs' and Class Members' Private Information.

175. A meeting of the minds occurred, as Plaintiffs and Class Members agreed, *inter alia*, to provide accurate and complete Private Information to Zeroed-In in exchange for Zeroed-In's agreement to, *inter alia*, provide services that included protection of their highly sensitive Private Information.

176. Plaintiffs and Class Members have been damaged by Zeroed-In's conduct, including the harms and injuries arising from the Data Breach now and in the future, as alleged herein.

COUNT V
UNJUST ENRICHMENT
(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS)

177. Plaintiffs restate and reallege the allegations in paragraphs 1 to 121 as if fully set forth herein.

178. This Count is pleaded in the alternative to Counts III and IV above.

179. Plaintiffs and Class Members conferred a benefit on Zeroed-In by turning over their Private Information, directly or indirectly, to Defendant in exchange for services that should have included cybersecurity protection to protect their Private Information. Plaintiffs and Class Members did not receive such protection.

180. Upon information and belief, Zeroed-In funds its data security measures entirely from its general revenue, including from payments made to it by Plaintiffs' and Class Members' employers.

181. As such, a portion of the payments made by Plaintiffs' and Class Members' employers is to be used to provide a reasonable and adequate level of data security that is in compliance with applicable state and federal regulations and industry standards, and the amount of the portion of each payment made that is allocated to data security is known to Zeroed-In.

182. Zeroed-In has retained the benefits of its unlawful conduct, including the amounts of payment received from Plaintiffs and Class Members that should have been used for adequate cybersecurity practices that it failed to provide.

183. Zeroed-In knew that Plaintiffs and Class Members conferred a benefit upon it, which Zeroed-In accepted. Zeroed-In profited from these transactions and used the Private Information of Plaintiffs and Class Members for business purposes, while failing to use the payments it received for adequate data security measures that would have secured Plaintiffs' and Class Members' Private Information and prevented the Data Breach.

184. If Plaintiffs and Class Members had known that Zeroed-In had not adequately secured their Private Information, they would not have agreed to provide such Private Information to Defendant.

185. Due to Zeroed-In's conduct alleged herein, it would be unjust and inequitable under the circumstances for Zeroed-In to be permitted to retain the benefit of its wrongful conduct.

186. As a direct and proximate result of Zeroed-In's conduct, Plaintiffs and Class Members have suffered, and/or are at a continued, imminent risk of suffering, injury that includes but is not limited to the following: (i) actual identity theft; (ii) the loss of the opportunity to control

how their Private Information is used; (iii) the compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their Private Information, which remains in Zeroed-In's possession and is subject to further unauthorized disclosures so long as Zeroed-In fails to undertake appropriate and adequate measures to protect Private Information in its continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

187. Plaintiffs and Class Members are entitled to full refunds, restitution, and/or damages from Zeroed-In and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Zeroed-In from its wrongful conduct. This can be accomplished by establishing a constructive trust from which the Plaintiffs and Class Members may seek restitution or compensation.

188. Plaintiffs and Class Members may not have an adequate remedy at law against Zeroed-In, and accordingly, they plead this claim for unjust enrichment in addition to, or in the alternative to, other claims pleaded herein.

COUNT VI
DECLARATORY JUDGMENT
(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS)

189. Plaintiffs restate and reallege the allegations in paragraphs 1 to 121 as if fully set forth herein.

190. Under the Declaratory Judgment Act, 28 U.S.C. § 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and to grant further necessary relief. Furthermore, the Court has broad authority to restrain acts that are tortious and violate the terms of the federal laws and regulations described in this Complaint.

191. Zeroed-In owes a duty of care to Plaintiffs and Class Members, which required it to adequately secure Plaintiffs' and Class Members' Private Information.

192. Zeroed-In still possesses Private Information regarding Plaintiffs and Class Members.

193. Plaintiffs allege that Zeroed-In's data security measures remain inadequate. Furthermore, Plaintiffs continue to suffer injury as a result of the compromise of their Private Information and the risk remains that further compromises of their Private Information will occur in the future.

194. Under its authority pursuant to the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Zeroed-In owes a legal duty to secure its clients' employees' Private Information and to timely notify customers of a data breach under the common law and the FTCA;

b. Zeroed-In's existing security measures do not comply with its explicit or implicit contractual obligations and duties of care to provide reasonable security procedures and practices that are appropriate to protect employees' Private Information; and

c. Zeroed-In continues to breach this legal duty by failing to employ reasonable measures to secure employees' Private Information.

195. This Court should also issue corresponding prospective injunctive relief requiring Zeroed-In to employ adequate security protocols consistent with legal and industry standards to protect employees' Private Information, including the following:

a. Order Zeroed-In to provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members.

b. Order that, to comply with Defendant's explicit or implicit contractual obligations and duties of care, Zeroed-In must implement and maintain reasonable security measures, including, but not limited to:

i. engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Zeroed-In's systems on a periodic basis, and ordering Zeroed-In to promptly correct any problems or issues detected by such third-party security auditors;

ii. engaging third-party security auditors and internal personnel to run automated security monitoring;

iii. auditing, testing, and training its security personnel regarding any new or modified procedures;

iv. segmenting its user applications by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of Zeroed-In's systems;

v. conducting regular database scanning and security checks;

vi. routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

vii. meaningfully educating its clients' employees about the threats they face with regard to the security of their Private Information, as well as the steps they should take to protect themselves.

196. If an injunction is not issued, Plaintiffs will suffer irreparable injury and will lack an adequate legal remedy to prevent another data breach at Zeroed-In. The risk of another such breach is real, immediate, and substantial. If another breach at Zeroed-In occurs, Plaintiffs will not have an adequate remedy at law because many of the resulting injuries are not readily quantifiable.

197. The hardship to Plaintiffs if an injunction does not issue exceeds the hardship to Zeroed-In if an injunction is issued. Plaintiffs will likely be subjected to substantial, continued identity theft and other related damages if an injunction is not issued. On the other hand, the cost of Zeroed-In compliance with an injunction requiring reasonable prospective data security measures is relatively minimal, and Zeroed-In has a pre-existing legal obligation to employ such measures.

198. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing a subsequent data breach at Zeroed-In, thus preventing future injury to Plaintiffs and other clients' employees whose Private Information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and the Class described above, seek the following relief:

a. An order certifying this action as a Class action under Fed. R. Civ. P. 23, defining the Class as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiffs are proper representatives of the Nationwide Class requested herein;

b. Judgment in favor of Plaintiffs and Class Members awarding them appropriate monetary relief, including actual damages, statutory damages, equitable relief, restitution, disgorgement, and statutory costs;

c. An order providing injunctive and other equitable relief as necessary to protect the interests of the Class as requested herein;

d. An order instructing Zeroed-In to purchase or provide funds for lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members;

e. An order requiring Zeroed-In to pay the costs involved in notifying Class Members about the judgment and administering the claims process;

f. A judgment in favor of Plaintiffs and Class Members awarding them prejudgment and post-judgment interest, reasonable attorneys' fees, costs, and expenses as allowable by law; and

g. An award of such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs demand a trial by jury on all triable issues.

DATED: December 4, 2023.

Respectfully submitted,

/s/ Jessica Wallace

Jessica Wallace (Bar No. 1008325)
SIRI & GLIMSTAD LLP
20200 West Dixie Highway, Suite 902
Aventura, FL 33180

T: (786) 244-5660
E: jwallace@sirillp.com

Mason A. Barney (*pro hac vice* to be filed)
Tyler J. Bean (*pro hac vice* to be filed)
SIRI & GLIMSTAD LLP
745 Fifth Avenue, Suite 500
New York, New York 10151
Tel: (212) 532-1091
E: mbarney@sirillp.com
E: tbean@sirillp.com